

Monthly news - December 2023


 techcommunity.microsoft.com/t5/microsoft-defender-xdr-blog/monthly-news-december-2023/ba-p/3998431

Microsoft Defender XDR Monthly news December 2023 Edition



This is our monthly "What's new" blog post, summarizing product updates and various new assets we released over the past month across our Defender products. In this edition, we are looking at all the goodness from November 2023.

Legend:

 Product videos	 Webcast (recordings)	 Docs on Microsoft	 Blogs on Microsoft
 GitHub	 External	 Product improvements	 Previews / Announcements

Microsoft Defender XDR

Introducing a **Unified Security Operations Platform with Microsoft Sentinel and Defender XDR**. An exciting private preview that represents the next step in the SOC protection and efficiency journey by bringing together the power of Microsoft Sentinel, Microsoft Defender XDR and Microsoft Security Copilot into a unified security operations platform with one experience, one data model and unified features, all enhanced with more AI, automation, attack disruption and curated recommendations.

In this video, Rob Lefferts, CVP Microsoft Threat Protection, joins Mechanics host Jeremy Chapman to discuss how the Defender experience has evolved into a unified security operations platform that combines threat detection, prevention, investigation, and response.

Ignite news: XDR in an era of end-user-to-cloud cyberattacks and securing the use of AI. This blog describes additional exciting Ignite news.

This Ninja Show episode summarizes the Security announcements:

Public preview of **Microsoft Defender for Cloud to Defender XDR integration**. (Preview) Microsoft Defender for Cloud alerts are now integrated in Microsoft Defender XDR. Defender for Cloud alerts are automatically correlated to incidents and alerts in the Microsoft Defender XDR portal and cloud resource assets can be viewed in the incidents and alerts queues. Learn more about the Defender for Cloud integration in Microsoft Defender XDR. Learn more on our docs.

Get email notifications for any actions in Defender XDR. This enables the SOC and relevant stakeholders (e.g., security admins, IT) to receive notifications whenever an automated or manual action is taken.

If you missed any of the **Virtual Ninja Show episodes**, you can **watch them all in this YouTube playlist**.

Upcoming episodes are listed on the show page: <https://aka.ms/NinjaShow>

Microsoft Security Experts

What's new in Microsoft Defender Experts for XDR. Learn more about the latest enhancements to the Defender Experts for XDR service, including customized managed response, API integration for third party SIEM/case management tools, a new Teams app, expedited onboarding, and a new Defender Experts banner on the Microsoft Defender home page.

Defender Experts for XDR now lets you **perform your own readiness assessment** when preparing the environment for the Defender Experts for XDR service.

Defender Experts for Hunting now lets you **generate sample Defender Experts Notifications** so you can start experiencing the service without having to wait for an actual critical activity to happen in your environment. Learn more [on our docs](#).

Microsoft Defender for Endpoint

The Defender for Endpoint plug-in for Windows Subsystem for Linux is now in public preview. This plug-in enables Defender for Endpoint to provide more visibility into all running WSL containers, by plugging into the isolated subsystem.

Microsoft Defender Core service is now available for consumers and is planned to begin rolling out to enterprise customers in early 2024. Learn more about it [on our docs](#).

Simplified security settings management is now generally available (GA).

What's new with the :

- **Streamlined security settings management in the Defender portal** by removing the dependency on the Microsoft Intune admin center.
 - **Native support for Linux, and macOS** by removing the dependency on 3rd party tools.
 - **Easy and reliable device enrollment** by removing the dependency on Microsoft Entra ID.
-

Mixed licensing for Defender for Endpoint is now generally available. Read the [previous announcement blog](#) for details.

Defender for Endpoint **P1 is now supported for US Government customers.**

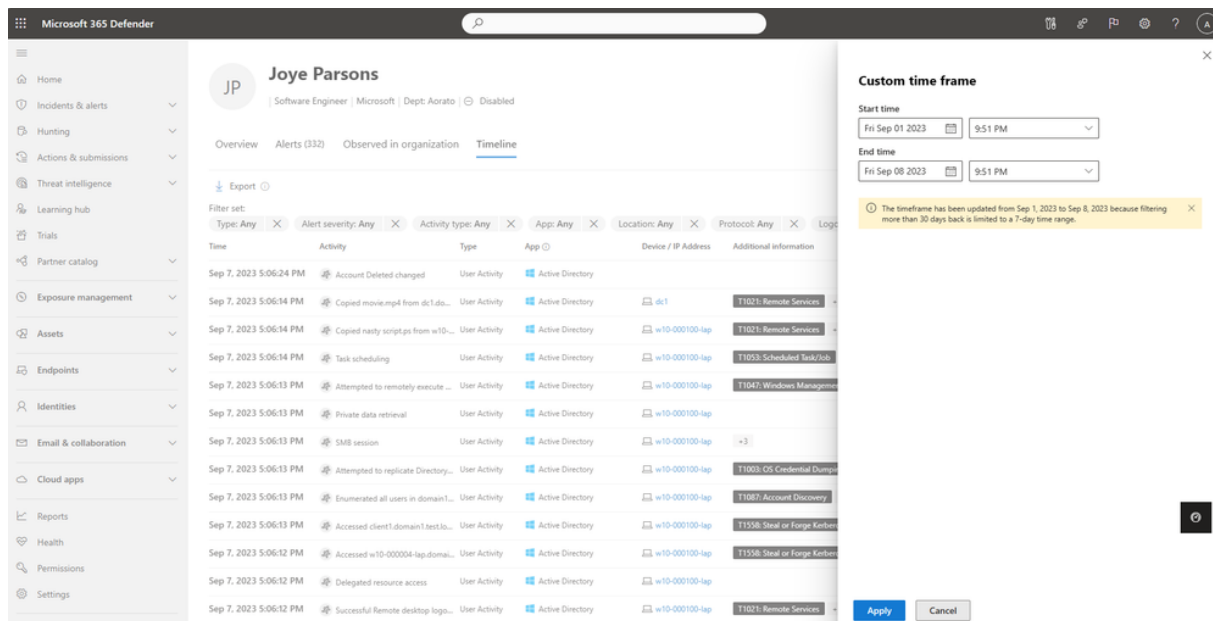
Microsoft Defender for Identity

Identity timeline includes more than 30 days of data (Preview).

Defender for Identity is gradually rolling out extended data retentions on identity details to more than 30 days.

The identity details page Timeline tab, which includes activities from Defender for Identity, Defender for Cloud Apps, and Defender for Endpoint, currently includes a minimum of 150 days and is growing. There might be some variation in data retention rates over the next few weeks.

To view activities and alerts on the identity timeline within a specific time frame, select the defa.... Filtered data from more than 30 days ago is shown for a maximum of 7 days at a time.



Screenshot showing the custom time frame filter

Microsoft Defender for Cloud Apps

New cloud app catalog category for Generative AI. The Defender for Cloud Apps app catalog now supports the new Generative AI category for large language model (LLM) apps, like Microsoft Bing Chat, Google Bard, ChatGPT, and more. Together with this new category, Defender for Cloud Apps has added hundreds of generative AI-related apps to the catalog, providing visibility into how generative AI apps are used in your organization and helping you manage them securely.

Test mode for admin users (Preview). As an admin user, you might want to test upcoming proxy bug fixes before the latest Defender for Cloud Apps release is fully rolled out to all tenants. To help you do this, Defender for Cloud Apps now provides a test mode, available from the Admin View toolbar.

General availability for more discovery Shadow IT events with Defender for Endpoint. Defender for Cloud Apps can now discover Shadow IT network events detected from Defender for Endpoint devices that are working in the same environment as a network proxy. Customers will now see Shadow IT data from endpoint devices which are behind a network proxy as well.

Microsoft Defender for Office 365

Create and manage simulations **using the Graph API in Attack simulation training.** The Graph APIs v1 to create/manage attack simulations is now generally available.

Enhanced Action experience from Email Entity/ Summary Panel. We added the ability for you to take multiple actions together. You can take email remediation actions, create submissions, tenant level block actions (block senders, domains, files, and URLs), investigative actions, and proposed remediation from the same panel.

Microsoft Defender for IoT

Enterprise IoT security is now included in Microsoft 365 E5 and E5 Security plans. To help organizations achieve a more holistic endpoint security strategy that traverses both IT and IoT devices easily, **we announced that the IoT security capabilities of Microsoft Defender for IoT are now included with Microsoft 365 E5 and E5 Security plans at no additional cost** for new and existing customers.

Microsoft Defender Vulnerability Management

Ability to request support for CVE. In case there a CVE which is not supported by Defender Vulnerability Management and is critical for your organization, you have the option to submit CVE support.
To see the new option, please navigate to 'Weaknesses', search for the CVE. If the CVE is not supported, you will have the below option:

The screenshot shows the Microsoft Defender Vulnerability Management interface. On the left, a list of CVEs is displayed with columns for Name and Severity. CVE-2023-6125 is selected. The main panel shows details for CVE-2023-6125, including a message indicating it is not supported and a button to request support. The vulnerability description, threat insights, and vulnerability details are also visible.

Name	Severity
CVE-2023-6131	High
CVE-2023-6130	High
CVE-2023-6128	Medium
CVE-2023-6127	Medium
CVE-2023-6126	Medium
CVE-2023-6125	Medium
CVE-2023-6124	Medium
CVE-2023-6111	High
CVE-2023-6099	Critical
CVE-2023-6098	Medium
CVE-2023-6097	Critical
CVE-2023-6084	Critical
CVE-2023-6076	Medium
CVE-2023-6075	Low

CVE-2023-6125

Open vulnerability page Report inaccuracy

Vulnerability details Related software

This CVE is currently not supported by Defender Vulnerability Management. If you are interested in obtaining information regarding this CVE, please indicate your request by selecting the 'Please support this CVE' button below. Your request will assist us in prioritizing this CVE among all others in our system.

[Please support this CVE](#)

Legal Notice The vulnerability data provided and shown as part of your Microsoft Defender for Endpoint (MDE) services is made available to you i...

Vulnerability description

Summary: The vulnerability is a code injection in the GitHub repository salesagility/suitecrm prior to versions 7.14.2, 7.12.14, and 8.4.2. This vulnerability allows a remote authenticated attacker to execute arbitrary code on the system.

Impact: If exploited, this vulnerability could allow an attacker to execute arbitrary code on the system, potentially leading to unauthorized access, data breaches, and further compromise of the affected system.

Remediation:... [Show more](#)

Threat insights

Public	Verified
No	No

Vulnerability details

Vulnerability name
CVE-2023-6125

Severity
Medium

CVSS
5.4 (lrm)

CVSS Version
3

Published on

Blogs on Microsoft Security

Social engineering attacks lure Indian users to install Android banking trojans. Microsoft has observed an ongoing spike in mobile malware targeting users in India in which scammers are using socially engineered phishing messages on WhatsApp and Telegram to lure users to install fake applications impersonating legitimate Indian banks, govt services, and utility apps.

Diamond Sleet supply chain compromise distributes a modified CyberLink installer. Microsoft uncovered a supply chain attack by the North Korea-based threat actor Diamond Sleet (ZINC) involving a malicious variant of an application developed by CyberLink Corp

Microsoft shares threat intelligence at CYBERWARCON 2023. Summary of what Microsoft is presenting at Cybewartcon

Threat Analytics Reports / Actor, activity & technique profiles (Portal access needed)

Activity profile: Lace Tempest exploits SysAid zero-day vulnerability. Beginning October 27, 2023, Microsoft Threat Intelligence observed the ransomware group Lace Tempest (DEV-0950) performing attacks on servers running the SysAid IT automation software, where Lace Tempest issued commands via the SysAid software to deliver a malware loader. Microsoft notified SysAid of the activity, who investigated and determined that there was a zero-day vulnerability in the SysAid on-premises software. SysAid quickly released an update addressing CVE-2023-47246, a path traversal vulnerability.

Vulnerability profile: CVE-2023-46604 vulnerability in Apache ActiveMQ. CVE-2023-46604 is a critical vulnerability in Apache ActiveMQ, an open-source message broker. Exploitation could allow remote attackers to launch commands. Public exploitation code is available, and Microsoft Threat Intelligence and other security researchers have identified attacks exploiting this vulnerability to deliver HelloKitty ransomware.

Vulnerability profile: CVE-2023-36033 in Windows Desktop Window Manager. CVE-2023-36033 is an elevation of privilege vulnerability in the Windows Desktop Window Manager (DWM) Core Library. This vulnerability could allow an adversary with access to a vulnerable environment to gain unauthorized privileged access. Microsoft released a patch on November 14, 2023.

Tool profile: Impacket. Impacket is a collection of open-source Python classes designed for working with network protocols. This tool is maintained by Fortra's Core Security and has become popular with adversaries due to ease of use and wide range of capabilities.

Actor profile: Pearl Sleet. The actor Microsoft tracks as Pearl Sleet (LAWRENCIUM) is a nation state activity group based out of North Korea that has been active since at least 2012. Pearl Sleet is known to primarily target defectors from North Korea, digital, print and broadcast media, and religious organizations, particularly in East Asia.

Vulnerability profile: CVE-2023-22518 vulnerability in Atlassian Confluence Server and Data Center. In early November 2023, Microsoft researchers observed the exploitation of CVE-2023-22518, a pre-authentication vulnerability that affects all unpatched versions of Atlassian Confluence Server and Data Center. Multiple adversaries have successfully exploited this vulnerability, including Storm-0062 – an actor Microsoft tracks that has previously been known to attempt exploiting Confluence vulnerabilities.

Actor profile: Storm-0365. The actor that Microsoft tracks as Storm-0365 (DEV-0365) is an infrastructure as a service (IaaS) layer directly managed by, or is in a business relationship with, Periwinkle Tempest (also known as Trickbot LLC) for use as command and control (C2) domains and servers.

Activity profile: Diamond Sleet supply chain compromise distributes a modified CyberLink installer. Microsoft Threat Intelligence detected a malicious variant of an application developed by the multimedia software company CyberLink Corp being downloaded from CyberLink's infrastructure. The malicious file, detected as LambLoad, was developed by the North Korea-based threat actor Microsoft tracks as Diamond Sleet (ZINC).

Activity profile: Iranian MOIS operators opportunistically deploy limited-impact wiper in response t... In late October 2023, operators associated with Storm-0842, an Iran-based group with ties to the Ministry of Intelligence and Security (MOIS), deployed a destructive payload known as the Bibi wiper, in an Israeli organization. This organization was previously compromised by Storm-0861, another Iranian group with ties to the MOIS, suggesting these groups might have collaborated. Storm-0842's use of the Bibi wiper appeared to be part of an opportunistic attack with limited impact.

Actor profile: Hazel Sandstorm. Hazel Sandstorm is a composite name used to describe several subgroups of activity assessed to have ties to Iran's Ministry of Intelligence and Security (MOIS), the primary civilian intelligence agency in Iran. Hazel Sandstorm operators are known to pursue targets in the public and private sectors in Europe, the Middle East, and North America. In past operations, Hazel Sandstorm has used a combination of custom and commodity tools in their intrusions, likely as a means of gathering intelligence to support Iranian national objectives.